Europäisches Patentamt | European Patent Office | Office européen des brevets

PCT/IB04/4156

Bescheinigung Certificate Attestation

Die angehefteten Unterlagen stimmen mit der ursprünglich eingereichten Fassung der auf dem nächsten Blatt bezeichneten europäischen Patentanmeldung überein.

The attached documents are exact copies of the European patent application described on the following page, as originally filed.

Les documents fixés à cette attestation sont conformes à la version initialement déposée de la demande de brevet européen spécifiée à la page suivante.

Patentanmeldung Nr. Patent application No. Demande de brevet n°

03293218.8

PRIORITY DOCUMENT

SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

Der Präsident des Europäischen Patentamts;
Im Auftrag

For the President of the European Patent Office

Le Président de l'Office européen des brevets
p.o.

R C van Dijk

Anmeldung Nr:
Application no.: 03293218.8
Demande no:

Anmeldetag:
Date of filing: 18.12.03
Date de dépôt:

Anmelder/Applicant(s)/Demandeur(s):

SCHLUMBERGER Systèmes
50, avenue Jean Jaurès
92120 Montrouge
FRANCE

Bezeichnung der Erfindung/Title of the invention/Titre de l'invention:
(Falls die Bezeichnung der Erfindung nicht angegeben ist, siehe Beschreibung.
If no title is shown please refer to the description.
Si aucun titre n'est indiqué se referer à la description.)

Dispositif portable

In Anspruch genommene Priorität(en) / Priority(ies) claimed /Priorité(s) revendiquée(s)
Staat/Tag/Aktenzeichen/State/Date/File no./Pays/Date/Numéro de dépôt:

Internationale Patentklassifikation/International Patent Classification/
Classification internationale des brevets:

G06K9/00

Am Anmeldetag benannte Vertragstaaten/Contracting states designated at date of filing/Etats contractants désignées lors du dépôt:

AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LU MC NL
PT RO SE SI SK TR LI

Bemerkungen:
Remarks:
Remarques:

The application was transferred from the above mentioned original applicant to:
Axalto S.A - Montrouge/ FR
The registration of the changes has taken effect on 29.07.2004

Dispositif portable

1 Etat de l'art

La présente invention décrit un concept qui se décline à travers la combinaison de nombreuses technologies. Pour répondre à ce concept, nous allons balayer les besoins et la manière dont ces derniers sont utilisés aujourd'hui.

1.1 La problématique

Le but de l'invention est de répondre aux besoins d'un fournisseur global de services (« Services Agregator »). Au sein de la vie quotidienne, nous sommes entourés de multiples services, du taxi qui vous transporte à la gare en passant par la compagnie de chemin de faire qui le relaie pour atteindre une destination plus lointaine et du traiteur qui vous vendra un sandwich pour le voyage. Pour chaque service, vous avez un opérateur (qui peut se limiter à un individu) qui délivre un service suivant des règles explicites (un tarif affiché) ou implicites liées à un contrat ou à des lois.

Certains opérateurs de réseau ont une action transversale à plusieurs métiers et fédère des acteurs locaux. Pour citer un des opérateurs transversaux, VISA et Matercard fédèrent des banques nationales et consolident de multiples paiements liés à la fourniture d'un service (Boulanger, Taxi, Cinéma,...) vers la banque du porteur. Dés lors, que l'opérateur de réseau à un accès à l'usager final, il peut par sa position, jouer l'intermédiaire vers d'autres fournisseurs de services que ceux qu'il fournit. Pour exemple, il est courant de voir des banquiers proposer des contrats d'assurance à leurs clients.

Pour être éligible à ce rôle, l'opérateur de réseau doit posséder certaines qualités :

- Il doit être totalement disponible.
- Posséder une image de confiance et de professionnalisme.
- Ces règles doivent être claires et accessibles à la compréhension de chacun.
- Il doit garantir la confidentialité des informations que son client lui confit et agir au mieux des intérêts de son client.
- Il doit être largement déployé sur la zone d'action de son client.

Tout opérateur de services, dispose d'un vecteur qui le représente. Par exemple, ce vecteur peut être un billet de d'avion pour une compagnie aérienne, une carte bancaire pour une

banque ou une carte SIM pour opérateur de téléphonie mobile. Ce vecteur doit supporter virtuellement l'ensemble des qualités que l'usager prête à l'opérateur de service.

A travers, ces règles nous déduisons un certain nombre de caractéristique que le vecteur de l'opérateur de services doit garantir :

- **Sécurité :** Le vecteur doit pouvoir fonctionner sans danger pour l'usager et garantir la sécurité d'accès aux services limitée au porteur du vecteur ou ayant droits (sous sa délégation). Le vecteur doit se protéger contre toutes attaques permettant l'accès aux services sans l'agrément de l'usager légitime.

- **Confidentialité :** Le vecteur donne accès a des données privées du porteur. Le vecteur est personnel et l'usager doit s'identifier vis-à-vis du vecteur pour accéder aux services.

- **Portabilité :** L'usager doit pouvoir accéder au service où qu'il soit. Idéalement, l'usager porte le vecteur. Le vecteur doit être petit et léger.

- **Connectivité :** Les services étant distribués sur la zone d'activité de l'usager avec une dynamique très importante allant de l'enveloppe corporelle de l'usager à une couverture mondiale. La connectivité peut être assurée directement ou indirectement suivant la distance entre l'usager et le service. La qualité de service est étroitement liée aux moyens de connexion, aussi la réactivité dudit moyen de connexion doit être compatible avec le service (ex. le video streaming implique une bande passante conséquente, le paiement à la volée réclame une réactivité et une bande passante adéquates (métro)).

- **Disponibilité :** Le vecteur de service doit être disponible en permanence ou son indisponibilité doit être négligeable en regard des services attendus. L'autonomie de fonctionnement doit couvrir la plage de temps d'accès au service.

- **Non répudiable :** Certains actes finalisés ne doivent pas être répudiables par l'usager aussi le vecteur de l'opérateur doit fournir des moyens afin d'assurer cette caractéristique. Qui dit acte, dit agrément aussi l'initialisation d'un service doit se traduire par une action formelle (ex : signature d'un acte de vente chez son notaire)

- **Authentique :** Le vecteur doit pouvoir prouver son authenticité et mettre en œuvre des moyens techniques pour bloquer sa duplication.
- **Simplicité :** Pour que le service soit accessible à la multitude, les moyens mise en œuvre doivent être à la portée de tous, suivrent les règles les plus élémentaires d'ergonomie et être le plus naturels possibles. Simple, rapide et naturel sont conjugués au sein de ce paragraphe.

Fort de ces règles, il est aisé de reconnaître certains de nos vecteurs de services à commencer par un simple billet de banque qui remplit, dans la mesure du service qu'il rend, le cahier des charges.

Plusieurs solutions existent aujourd'hui pour répondre à l'ensemble du cahier des charges dans un domaine d'activité donnée. Aussi, plusieurs vecteurs sont déployés par des opérateurs pour couvrir leurs domaines :

- Une carte bancaire pour les banques.
- Une carte SIM pour un opérateur de téléphonie mobile.
- Un billet de banque ou un passeport pour un pays.
- Un reçu de pressing pour un service de nettoyage.
- Une clé pour un fabriquant de serrure.

Il va de soi que les règles qui régissent ces vecteurs sont modulés en fonction de la valeur du service ou de l'image de l'opérateur. Ainsi la valeur d'un ticket de pressing est limitée par contrat et les moyens pour garantir la sécurité sont limités. Une carte bancaire donne accès à des valeurs plus importantes aussi l'accent sur la non-répudiation, l'authenticité sera renforcée. Finalement, des vecteurs de petites valeurs intrinsèques (un billet de 10 €) peuvent porter une image importante (confiance dans un moyen de paiement supporté par un pays).

Un opérateur d'agrégation de service doit endosser l'ensemble des caractéristiques des sous-opérateurs qu'il doit agréger au sein d'un vecteur unique.

La présente invention décrit le vecteur de cet opérateur que nous appellerons eGo (en latin : moi). La fonction d'eGo est de servir un usager unique qui devient une « ordonnance (aide de camp) virtuelle » et qui consolide l'ensemble des services. eGo devient le représentant physique d'agrégation de services qui canalise l'information utile vers des moyens de traitement adéquats.

1.2 Inconvénients

Le manque d'universalité est la carence principale des vecteurs que les opérateurs de services ont poussés. Pour principalement des raisons économiques, les vecteurs ont été spécialiser pour leur domaine (ex. un ticket de métro). Nous pourrions imaginer l'utilisation de la carte à puce comme vecteur universel où au lieu d'un ticket de pressing, un employé vous donnerait une carte à puce ; mais visiblement, ce vecteur ne répond pas de façon autonome ou économique à l'ensemble des règles que nous avons édictées précédemment.

Par ailleurs, le vecteur est généralement transmis physiquement ou détruit après la complétion ou l'initialisation du service. Par exemple, le billet de banque est transmis contre une course en taxi et le billet de cinéma est déchiré après l'entrée dans la salle de spectacle. Dans les deux cas, le mode de transfert de valeur implique :

Une masse de vecteurs en circulation supérieure à la valeur des services (e.g. masse monétaire) et un coût de gestion/remplacement (usure) importante.

Des consommables et des coûts de personnalisation (impression d'un ticket de métro vierge. Ceci répond indirectement au besoin de non-duplication (contrefaçon) et d'acte d'agrément.

Par ailleurs, la complétion d'un service passe par plusieurs phases qui réduisent l'efficacité. Pour exemple, si l'usager désire voir un film dans une salle de cinéma, il doit :

- Se présenter à une caisse.
- Acheter un billet en contre-partie d'un moyen de paiement
- Prendre son billet
- Donner son billet à un employé de salle qui le déchirera

Idéalement, l'usager devrait pousser la porte de la salle de cinéma, voir son film et repartir sans jamais interagir avec qui ou quoi que cela soit.

Nous concluons notre analyse de l'état de l'art qui se traduit par une multitude de solution sans interaction ou assez peu en regard du besoin exprimé par un opérateur global qui souhaiterait consolider en ensemble de services variés fournis par d'autres.

1.3 Invention

La présente invention est un objet portable, que nous appellerons eGo et qui par certains aspects reprend les caractéristiques d'une carte à microprocesseur, et apte à supporter une portion non négligeable des qualités essentielles du vecteur de l'opérateur de services.

Trois moyens ont été ajoutés pour assurer l'ensemble des qualités requises. La combinaison et le choix de ses moyens portent la valeur inventive de la solution.

1.3.1 Principe de l'invention

L'invention est un principe de combinaison de moyen de communication aux propriétés différentes qui permet d'établir une communication à grande vitesse, fiable et courte portée (< 3m) entre deux équipements :

- Le premier équipement est personnel et son usager s'est identifié auprès de lui : eGo (l'invention).
- Le second est un équipement tiers apte à communiqué avec eGo.

Les deux équipements peuvent établir une communication privée à la condition absolue que l'usager touche physiquement l'équipement tiers avec une partie quelque conque de son corps. Pour se faire, le corps humain est utilisé comme médium de communication pour porter un signal de l'équipement tiers jusqu'à l'invention (eGo).

L'équipement tiers dispose d'un émetteur de communication à travers la peau (OSC : Over Skin Communication) et d'un émetteur RF (Radio Fréquence) à grande bande passante. eGo possède le pendant de l'équipement tiers à savoir : un récepteur OSC et un transmetteur RF. Pour établir une communication entre les deux équipements, trois étapes sont nécessaires :

1. L'équipement tiers envoie à eGo un code liaison composé de deux nombres aléatoires A, B et d'un message C par le truchement de son émetteur OSC. Le message C contient un identifiant de classe de l'équipement tiers.
2. Le récepteur OSC d'eGo reçoit le code de liaison, garde le nombre A et publie B grâce à son transmetteur RF qui si eGo est abonné à la classe (message C) de l'équipement tiers.
3. Le transmetteur tiers établi un canal sécurisé avec l'équipement eGo qui publie le nombre B et demande le nombre A pour comparaison à l'équipement eGo. Une fois la communication établie, deux nouveaux nombres aléatoires A et B sont tirés pour ouvrir une nouvelle connexion.

La solution présente initialement deux avantages :

- Sécuritaire : les ressources d'eGo ne peuvent être utilisées que si son porteur touche physiquement un équipement. Ceci interdit l'utilisation abusive d'eGo sans un agrément semi- formel de son porteur pleinement identifié.

- Persistance : Bien que le contact soit furtif (touché) avec l'équipement tiers, une communication fiable est rapide persiste entre lesdits équipements dans la limite des transmetteurs RF.

Cette technique permet de conserver les avantages d'une communication de type OSC (agrément et utilisation personnel d'un réseau d'équipement de proximité) sans les inconvénients (faibles débits de transmission).

Une fois la session de communication RF ouverte, les deux équipements peuvent à loisir échanger des messages pour compléter :

- Une transaction (ex : paiement),
- Une authentification unilatérale/mutuelle grâce à des moyens cryptographiques (ex. PKI),
- Un transfert de donnée,
- ...

A noter que la communication RF peut être chiffrée et utilisée un standard d'interopérabilité (ex : IETF- TLS) et un protocole de communication standard du type TCP/IP.

Nous comprendrons à travers ce document que d'autres avantages sont apportés par l'invention.

Pour éviter l'usage d'eGo sans l'autorisation formelle de son propriétaire, un dispositif d'identification biométrique est embarqué au sein d'eGo. Cette identification formelle est nécessaire à la mise en service d'eGo ou chaque fois qu'une identification formelle explicite est réclamée par l'équipement tiers (ex. un acte de paiement).

En contrepartie du système d'identification d'eGo, un système concurrent détecte la présence de corps de l'usager afin de désactiver eGo si celui-ci est séparé. Plusieurs détecteurs de signes vitaux non invasifs sont possibles pour remplir cette fonction [ANI02]. Pour exemple, des cardiotachymètre sont aujourd'hui embarqués dans des montres de sport.

Notre invention est en résumé capable de porter à proximité immédiate des services personnelles à fortes valeurs ajoutés de manière sécurisée en environnent multiples (hostiles ou sécurisés).

La figure 1 illustre l'environnement immédiat d'eGo.

Par ailleurs, un système de mesure de temps embarqué dans eGo permet de traiter des services impliquant une mesure de temps ou de l'horodatage (ex. Digital Rights Management).

1.3.2 Description de l'invention

L'invention est caractérisée par :

- Un moyen de calcul (3) par le truchement d'un microcontrôleur caractérisé en ce qu'il dispose de moyens qui garantissent la confidentialité des données qu'il traite. Ledit microcontrôleur dispose sur un même microcircuit protégé contre les intrusions plusieurs interfaces de communications, à savoir :
  - Un bus de communication rapide avec une mémoire additionnelle. Ledit bus pourrait être choisi en fonction de la disponibilité des mémoires du marché. Le bus de communication mémoire est utilisé de manière interne à eGo aussi, l'interopérabilité avec un équipement externe à eGo n'est pas recherché. Le choix du bus de communication est principalement économique afin d'équiper eGo avec les mémoires les plus adéquates avec les objectifs marketing et techniques d'eGo. Pour exemple un bus série de type SPI (Serial Peripheral Interface) ou parallèle de type MMC (Multi Media Card) pourrait être utilisé.
  - Une interface de communication avec un récepteur de type Near Field Communication.
  - Une interface de communication avec un transmetteur RF à large bande passante.
  - Une interface avec capteur biométrique qui avantageusement pour être intégré au microcontrôleur.
- Un récepteur/démodulateur (4) de signaux issue d'un capteur couplé au corps de l'utilisateur que nous appellerons OSCR (Over Skin Communication Receiver). La description dudit OSCR sera détaillé plus avant dans le document. Ce récepteur doit être apte à recevoir une petite quantité d'information (quelques centaines de bits) sur une très courte distance (moins d'un centimètre) à travers un médium de communication qui est une partie du corps de l'usager. L'établissement de la communication de façon préférentielle un contact physique entre l'usager et un équipement autre qu'eGo.

- Une mémoire (2) non volatile additionnelle de capacité importante apte à sauvegarder les données privées de l'usager. Le contenu de la mémoire étant chiffré par le microcontrôleur sécurisé.

- Un émetteur/récepteur RF (5) à courte portée (<10 m) et grande bande passante. Cette fonction doit être capable d'assurer une couche de transport fiable de données avec une bande passante importante supérieure à 2 Mbits/s.

- Un moyen (6) d'identification de l'utilisateur d'eGo. De manière préférentielle, ce moyen est biométrique et peut être un capteur d'empreinte digital capacitif/thermique/optique ou une reconnaissance d'empreinte vocale. Cependant tous autres moyens pouvant être embarqués au sein d'eGo et assurant une fiabilité compatible avec le niveau de sécurité et de disponibilité d'eGo peuvent convenir.

- Une batterie, le moyen de la recharger par le truchement d'un jeu de contact ou par induction magnétique et un moyen pour mesurer la charge de ladite batterie.

- Un circuit d'horodatage sécurisé apte à pouvoir être réglé par le truchement d'un réseau de communication (Network Time Protocol : RFC 1119 et RFC 1305)

Optionnellement (ou légalement), eGo peut avantageusement disposer de deux fonctions supplémentaires :

- Un indicateur visuel (ex : une LED (diode électroluminescente) ou un afficheur LCD)

- Un micro buzzer.

C'est deux options permettent au porteur d'eGo de transmettre un quitus quant à la bonne identification du porteur d'eGo par eGo. L'option visuelle et/ou sonore de cette fonction permet d'adresser des porteurs à capacités réduites (sourd, aveugle) voire des individus évoluant dans des environnements difficiles (ex : bruyants).

L'ensemble de ces fonctions est contenu au sein d'un boîtier qui peut être avantageusement une montre et son bracelet, une ceinture ou un bijou dont le volume est apte à contenir l'ensemble des fonctions d'eGo.

La figure 2 donne une vue fonctionnelle d'eGo.

2 Détails des fonctions

2.1 Caractéristiques globales

Les fonctions intégrées dans l'invention ont en commun le souci de gérer l'énergie afin d'assurer la plus grande autonomie de l'invention. Par l'universalité des services que porte eGo, son importance et sa disponibilité sur une longue période d'activité sans rechargement de sa batterie sont essentiels. Les technologies qui garantissent une très basse consommation sont avantageusement sélectionnées pour la réalisation d'eGo.

2.2 L'unité de calcul

L'unité de calcul est confinée au sein d'un microcircuit électronique (référencé 3 dans la figure 2) afin de faciliter sa protection contre des attaques sécuritaires extérieures. Aussi les principes qui régissent la réalisation des cartes à microprocesseur sont intégralement repris.

L'unité de calcul est composée des fonctions suivantes :

- Un microprocesseur apte à assurer l'algorithmique et la gestion des ressources d'eGo (ressources et couche de communication).
- d'une mémoire vive (RAM),
- d'une mémoire interne non-volatile (E^2PROM, FLASH,...) apte à mémoriser des données en absence d'énergie (batterie vide),
- de capteurs de sécurité (sous tension, ...) aptes à détecter des attaques sécuritaires (lumieres, eBeam,...),
- d'une base de temps apte à mesurer l'heure et la date (horodateur),
- d'interfaces aptes à assurer la liaison avec les fonctions d'eGo extérieures au microcircuit (3),
- de coprocesseurs optionnelles aptes à accélérer/améliorer certains algorithmes qui serait coûteux en temps ou en énergie si ces derniers devait

être réalisés par logiciels (ex : crypto-processeur, ECC (Error Code Correction), ...),

- de moyens de protection contre les investigations électroniques (DPA, DFA, EMC).

2.3 Le transmetteur RF

Le transmetteur RF est choisi de manière à assurer les qualités suivantes :

- Faible consommation (inférieure à 20 mW en émission et réception),
- Bande passante entre 2Mbits/s et 100 Mbits/s suivant les domaines que doit couvrir eGo.
- Modulation à étalement de spectre directe (Direct Spread Spectrum System) afin de limiter la sensibilité du transmetteur aux interférences.
- Temps d'établissement du canal de communication court (< 5 ms).
- Courte portée (inférieure à 10 m)
- Faible puissance d'émission (inférieure à 1 mW).

La technique d'étalement de spectre peut-être résumé simplement.

Voir figure 3.

Pour réaliser cette fonction il suffit de multiplier un signal de donnée par un code d'étalement.

Voir figure 4.

Plusieurs standards ou initiatives sont éligibles pour assurer cette fonction :

- Bluetooth (IEEE 802.15.1)
- WPAN (IEEE 802.15.3)
- Hiperlan2
- ETSI-BRAN

Seul Bluetooth est utilisable internationalement à la date de la rédaction de ce brevet pour des raisons de régulation. Les autres standards sont comparable et se regroupe sous la dénomination commune UWB (Ultra Wide Band).

Les caractéristiques techniques de l'UWB répondent aux critères requis par notre module de transmission RF hormis que la technologie n'est pas encore au rendez-vous quant à la consommation des produits existants (ex. XtremSpectrum produits « Trinity »). La consommation maximale est de 200 mW pour un débit de 100 Mbits/s.

Il est important de noter qu'une portée de notre transmetteur RF n'est pas recherchée bien au contraire. Pour limiter l'influence d'eGo à la périphérie immédiate de l'usager, la zone d'influence d'eGo doit être maîtrisée.

Par ailleurs, le protocole et le transmetteur doivent être capable de maintenir plusieurs communications simultanément.

Les premiers à avoir eu l'idée de ce système sont l'actrice autrichienne Hedy Lammar et le compositeur américain George Antheil, leur brevet a été déposé en 1942. L'actrice autrichienne, qui a fuit son pays à cause des événements politiques de l'époque, était très intéressée à la réalisation d'un système permettant la transmission de donnée de manière sûr afin de déjouer les plans allemands. Celui-ci a été utilisé par les militaires dès 1960. Il faut noter que l'UWB se prête très bien à la mesure de distance (ex : radars militaires et GPS) et peut être utilisé avantageusement dans une application d'eGo.

Aujourd'hui la plupart des moyens de transmissions modernes utilisent ce principe (ex. CDMA pour les mobiles ou WIFI (IEEE 802.11).

2.4 Le récepteur OSC

La transmission d'information à travers le corps humain (ou animal) est étudiée depuis le début des années 80. T. Zimmermann a décrit dans sa thèse [ZIM95] un réseau local limité (Personal Area Network) à un individu qui utilise sa masse biologique comme medium de transmission.

Le principe de transmission repose sur l'utilisation des champs quasi-électrostatiques. Le couplage entre le corps est principalement capacitif [GONZ01]. Pour assurer une transmission de donnée, il est nécessaire d'avoir un chemin de retour des courants générer par un transmetteur et transmis au medium biologique. La Terre est utilisée pour fournir le conducteur de retour.

La figure 5 illustre le principe dans la transmission.

Cette technique de transmission ne permet pas d'atteindre des débits de transmission importants [MAT97](< 10 KBits/s).

Le modèle électrique équivalent est donné dans la figure 6.

L'atténuation du signal émis par le transmetteur (T) est considérable (60 dB) et dépends principalement du retour par la terre (10fF). Le signal d'émission doit être assez puissant pour être correctement décodé par le récepteur (R) (environ 20 Vcc). Cependant un signal de moindre amplitude peut être choisi si le récepteur est plus sensible et la technique de modulation s'affranchie des interférences (ex : DSSS techniques).

Le schéma électronique simplifié est donné dans la figure 7

Le niveau d'émission et la faible consommation nécessaire par eGo imposent deux éléments de la solution :

- Le récepteur est coté eGo et pas l'inverse.
- Si le niveau d'émission est faible, le codage des informations transmises à eGo par ce médium doit utiliser avantageusement une technique à étalement de spectre (DSSS : Direct Sequence Spread Spectrum)

Le transmetteur est un simple générateur apte à transmettre via un couplage capacitif/résistif un code de liaison avec eGo.

La figure 8 illustre l'aspect fonctionnel de l'émetteur.

Le code de liaison avec eGo est étalé par le truchement d'un générateur de séquences, par exemple des séquences fixes (WIFI) appelées « Barker chip « sur n bits (11 pour WIFI) ou des TFSR (Tapped Feedback Shift Register ou GPA (générateur pseudo aléatoire)) qui est un registre à décalage rebouclé basé sur un polynôme premier ($X^{10}+X^3+1$ pour le GPS). Le code étalé est injecté dans un modulateur (FSK, FM ou AM) d'un générateur HF (porteuse).

Le code de liaison est partagé est généré par le sous-système que veut établir une liaison avec eGo.

Il est important de noter que la transmission OSC est unilatérale (de l'équipement tiers vers eGo et pas l'inverse) et elle n'est pas cryptée.

2.5 La batterie

La batterie doit présentée une capacité massique importante afin de minimiser le volume et le poids tout en assurant une disponibilité d'eGo compatible avec un usage intensif sans

rechargement. Les technologies de batterie développées pour les téléphones portables peuvent remplir le cahier des charges de l'invention.

Il faut noté que l'invention sera principalement en veille, seul le récepteur, l'horodateur et le capteur de signes vitaux sont partiellement actif. Une fois, les premières réceptions du code liaison via le récepteur OSC vont réveiller l'ensemble des fonctions d'eGo hormis le capteur d'identification biométrique qui ne sera activé que si le porteur d'eGo n'est pas identifié. La journée durant, le porteur d'eGo sera en contact avec une multitude d'équipement compatible avec le système eGo, afin de minimiser la consommation d'énergie, un filtrage par le bais de la classe de l'équipement tiers permet de ne pas activer la transmission RF si eGo n'est pas abonné à cette classe.

Une fois qu'eGo a activé une session de communication avec l'équipement tiers, cette session est vérifiée périodiquement (technique de « sniffing ») pour vérifier la proximité des équipements. Entre deux activation, seul le récepteur RF est partiellement actif.

Aucun contact électrique n'est requis pour recharger la batterie. Avantageusement et pour des raisons sécuritaires (EMI, Digital Fault Analysis), la recharge de la batterie est réalisée par induction magnétique. eGo embarque en son sein le secondaire d'un transformateur magnétique, le rechargement de la batterie se réalise en posant eGo sur un support qui contient le primaire du transformateur.

D'autres techniques de transfert d'énergie peuvent être utilisées comme la lumière avec un convertisseur basé sur des cellules photovoltaïques ou un champ electro-magnétique (HF) et une antenne pour la conversion.

Un dispositif de mesure de charge est intégré à eGo afin d'avertir son environnement que la batterie est presque déchargé ou totalement chargé. Cette mesure peut-être transmise vers un équipement extérieur à eGo via sa liaison RF vers un équipement tiers disposant d'une interface homme/machine adéquate (ex : PC ou le chargeur). Un eGo équipé d'un afficheur LCD (Liquid Crystal Display) ou OLED (Organic Light Emitted Diode) peut ergonomiquement relayer la jauge de charge de la batterie.

2.6 La mémoire additionnelle

Une mémoire additionnelle de forte capacité (jusqu'à plusieurs dizaines de Megaoctets) est connectée à l'unité de calcul. Le contenu de ladite mémoire est encrypté par un algorithme dont la clé secrète diversifiée est uniquement connue d'eGo. La communication avec l'unité de calcul est réalisée par le truchement d'un bus standard de type MMC (Memory Multimedia Card) , SPI ou tout autre bus compatible avec ce type de mémoire.

Cette mémoire est amenée à contenir des données privées telles que contrats de service, droits digitaux, données privées, photos et autres données administratives nécessaires si eGo ne peut être connecté à un réseau local ou mondial (ex. Internet).

3 Solution(s) apportée(s) par l'invention

L'invention apporte une solution évidente pour porter les services d'un opérateur de manière transparente et naturelle pour un usager. Les capacités de calcul, de stockage de données, de contrôle de positionnement/proximité, l'identification formelle du porteur, d'un agrément légal (quitus) de l'usager permettent à eGo d'être un vecteur universel pour un opérateur de service qui peut, à l'extrême, être limité à l'usager lui-même.

3.1 Applications d'eGo

Nous allons cités une liste non exhaustive d'applications reliées à eGo. Dans toutes les applications, il y a une interaction entre un sous-système (cf. dans la figure 1.) et eGo par un contact physique initial sur le représentant du sous-système labellé « @ » dans les paragraphes suivants ?

3.1.1 Téléphonie

eGo adresse simplement tout système de communication qui peut ainsi aisément et instantanément personnalisé au porteur d'eGo :

- **Mobile :** A l'instant ou le téléphone mobile® est saisi par un porteur d'eGo, le téléphone mobile est configuré et apte à recevoir des appels. Le répertoire téléphonique est accessible via l'interface Homme/Machine du téléphone et les préférences de l'usager sont appliquées. Si le téléphone est remis à une tierce personne, celui-ci devient son téléphone.
- **Fixe privée ou public :** Le fait de saisir un téléphone® permet d'accéder à son répertoire et de facturer l'appel sur son compte téléphonique et non celui de la personne où est disponible le téléphone.

3.1.2 Paiement

D'une façon très naturel, nous pouvons choisir un article (boisson, journal,...) dans un distributeur ouvrir le sas d'accès® à l'article et prendre l'article sans jamais avoir introduit monnaie ou carte de crédit dans ledit distributeur automatique.

Pour des montants importants, eGo peut transmettre la photo de son propriétaire afin que celui-ci puisse être authentifié par un caissier. Un agrément (quitus) par une identification formelle par le biais de capteur biométrique (ex : ATMEL) peut faire office de PIN code.

L'ensemble des transactions est automatique ou quasiment (agrément) et réalisé de manière naturelle, sans effort et à la portée de toutes personnes quel que soit sont ages et son éducation.

Un enfant équipé d'eGo aura la possibilité d'accéder à des services scolaires (ex : cantine,...) grâce aux service de paiement automatique que porte eGo et cela quelque soit sont age.

3.1.3 Accès conditionnel

Le paiement dynamique (le porteur est en mouvement) ou statique (porteur à l'arrêt) est possible simplement grâce à eGo :

- Accès à un équipement: Le fait de toucher un ordinateur® permet une identification d'usage et le chargement du profil de son utilisateur. Aucun mot de passe n'a été demandé. Si l'utilisateur s'éloigne, l'ordinateur peut automatiquement se verrouiller.
- Accès à un moyen de transport : eGo peut élégamment et naturellement jouer le rôle de clé d'automobile® et de support de documents administratifs associées (permis de conduire, assurance, contrat de location). eGo permet d'accéder à un moyen de transport en commun bus, métro en poussant simplement la porte® d'accès dudit moyen de transport. Le contrôle et le paiement sont réalisés dans les quelques mètres entre le porteur d'eGo et le sas d'accès. Par ailleurs, le paiement à la distance parcourue (métro, train) est possible simplement car il devient simple (capacité de géo-localisation d'eGo) de connaître le point d'entrée et de sortie dans un réseau de transport.
- Péage autoroutier : Une automobile® compatible eGo peut relayer les droits du conducteur équipé d'eGo. Le paiement est réalisé à la volée lors du passage du véhicule par eGo ou par le véhicule qui transférera le paiement vers eGo.
- Données personnelles : eGo permet le stockage de donnée privée avec un accès conditionnel automatique (utilisation avec un ordinateur) mais également public ou semi-public. eGo peut être utilisé pour stocker des données administratives (ex : passeport, carte d'identité) accessible par un personnel autorisé lui-même équipé d'un eGo (ex : fonctionnaire de police). eGo peut publier des données jugées publiques pour adresser des services variés comme (petites annonces, programme de fidélisation, enquêtes marketing, stockage de renseignements

techniques/publicitaires collecter dans un magasin sur des articles/rayons « eGo compliant »)

- Accès à des données: eGo permet de chiffrement et du déchiffrement à la volée ainsi que du stockage. Une icône dans un coins de l'écran de l'ordinateur® d'un porteur d'eGo permet de sélectionner un document et de le déplacer vers/dans/via eGo (Drag and Drop/ Glisser et lâcher)
- Accès à un lieu : La commande d'une serrure électrique ou l'inhibition d'une alarme peut être réaliser en tournant simplement la poignée® d'une porte.
- Pointeuse : eGo permet un pointage automatique dès que son porteur accède à la porte® de son entreprise, il lui suffit pour cela de pousser la porte d'accès.

3.1.4 Localisation /surveillance

eGo permet une localisation précise de part son principe (mieux que 30 cm de précision):

- **Surveillance** : Un enfant équipé d'eGo peut déclencher une alarme si ce dernier sort d'un périmètre autorisé (ex: école) dès qu'il touche un objet hors limite de ce périmètre (ex : portes®).
- **Localisation** : Un enfant équipé d'eGo peut se signaler et donner sa position exacte en touchant une borne® relais prévu à cet effet. Un message pourra être envoyé à ses parents avec les coordonnées exactes pour le trouver.
- **Enregistrement** : Une arme® à feu (ex : revolver) peut être compatible eGo, son propriétaire légitime est seul à pouvoir l'utiliser. Un équipement tiers activé peut être détecté dans une enceinte où l'équipement est illicite (ex : banque, avion,...) et déclenché une alarme et/ou un enregistrement vidéo.

4 Champ(s) d'application de l'invention

L'invention a un usage transversal à la plupart des activités humaines.

5 Produit(s)

Ladite invention est en dehors du contexte des cartes à microprocesseur. Aucune norme, ni facteurs de forme qui s'appliquent aux cartes à microprocesseur à contact ou sans contact ne s'appliquent à l'invention. L'invention peut être utilisée comme un produit de substitution de la carte à microprocesseur et la remplacer avec avantages. Cependant certaines techniques utilisés dans les cartes à microprocesseur liées à la sécurité (ex : DPA) pourront être utilisé avec avantage.

Revendications

1. Dispositif portable caractérisé en ce qu'il contient : une unité sécurisée de calcul et de mémorisation, un capteur biométriques d'identification, un récepteur de communication de type OSC, un transmetteur RF et une source d'énergie électrique autonome, et caractérisé en ce que le moyen de communication OSC est utilisé pour initier une session de communication RF.
2. Dispositif portable suivant la revendication 1 caractérisé en que le capteur biométrique est un capteur d'empreinte digitale
3. Dispositif portable suivant la revendication 1 caractérisé en que le capteur biométrique est un capteur d'empreinte vocale.
4. Dispositif portable suivant la revendication 1 caractérisé en que le capteur biométrique est un capteur d'empreinte digitale sous derme (ultrason)
5. Dispositif portable suivant la revendication 1 caractérisé en que le moyen de communication RF est du type UWB (Ultra Wide Band).
6. Dispositif portable suivant la revendication 5 caractérisé en que le moyen de communication RF est du type UWB et répond au standard IEEE802.15.1 (bluetooth)
7. Dispositif portable suivant la revendication 5 caractérisé en que le moyen de communication RF est du type UWB et répond au standard IEEE802.15.3 (WPAN).
8. Dispositif portable suivant la revendication 5 caractérisé en que le moyen de communication RF est du type UWB et répond au standard ETSI BRAN.
9. Dispositif portable suivant la revendication 5 caractérisé en que le moyen de communication RF est du type UWB et répond au standard HIPERLAN.
10. Dispositif portable suivant la revendication 1 caractérisé en que le moyen de communication OSC utilise une masse biologique comme medium de transmission (ex : peau).
11. Dispositif portable suivant la revendication 10 caractérisé en que le moyen de communication OSC utilise une technique de transmission à étalement de spectre (ex. DSSS).
12. Dispositif portable suivant la revendication 1 caractérisé en qu'il dispose d'un détecteur d'un signe vital apte à détecter la séparation physique dudit dispositif et de son porteur.

13. Dispositif portable suivant la revendication 1 caractérisé en qu'il dispose d'un détecteur d'un signe vital apte à détecter la séparation physique dudit dispositif et de son porteur.

14. Dispositif portable suivant la revendication 1 caractérisé en qu'il dispose d'un horodateur autonome.

15. Dispositif horodateur suivant la revendication 14 caractérisé en qu'il peut être paramétré à distance par l'accès à un réseau adéquat par un second horodateur sécurisé via un protocole de type NTP ou équivalent.

16. Dispositif portable suivant la revendication 1 caractérisé en ce qu'il dispose d'une interface homme/machine sonore ou visuel apte à transmettre un quitus au porteur dudit dispositif.

17. Interface homme/machine suivant la revendication 16 en ce que ledit dispositif de transmission de quitus est une LED (diode électroluminescente).

18. Interface homme/machine suivant la revendication 16 en ce que ledit dispositif de transmission de quitus est un micro buzzer.

19. Interface homme/machine suivant la revendication 16 en ce que ledit dispositif de transmission de quitus est un vibreur.

20. Source d'énergie électrique autonome caractérisée en ce qu'elle est rechargeable par un dispositif de transfert d'énergie sans contact galvanique.

21. Dispositif de transfert d'énergie caractérisé en ce qu'il utilise une induction magnétique comme medium de transfert d'énergie.

22. Dispositif de transfert d'énergie caractérisé en ce qu'il utilise la lumière comme medium de transfert d'énergie et des cellules photovoltaïques pour la conversion d'énergie.

23. Dispositif de transfert d'énergie caractérisé en ce qu'il utilise un champ électro-magnétque comme medium de transfert d'énergie et une antenne comme sous-système de conversion.

24. Dispositif portable suivant la revendication 1 caractérisé en que la transmission OSC est unilatérale et vers le dispositif.

25. Dispositif portable suivant la revendication 1 caractérisé en que la transmission OSC est non chiffrée.

26. Dispositif portable suivant la revendication 1 caractérisé en que le message transmis via le moyen de transmission OSC conditionne l'ouverture et le démarrage d'une session de communication RF.

27. Méthode d'ouverture de session suivant les revendications 1, 24,25 et 26 caractérisée en ce que le dispositif est capable de filtrer les équipements candidats à une ouverture de session de communication RF grâce à des informations transmises par le truchement de la communication OSC.

28. Méthode d'ouverture de session suivant la revendication 27 caractérisé en ce que les informations transmises via le communication OSC sont deux nombres aléatoires.

29. Méthode d'ouverture de session suivant la revendication 1 et 27 caractérisé en ce que les informations transmises via la communication OSC sont deux nombres aléatoires et un identifiant de classe d'équipements supportés par le dispositif 1.

30. Dispositif portable suivant la revendication 1 et 5 caractérisé en ce qu'il permet de localiser physiquement le porteur du dispositif dans un espace borné.

31. Dispositif portable suivant la revendication 30 caractérisé en ce que cette localisation est combinée avec les moyens d'identification cryptographique et/ou biométrique.

32. Disposer portable suivant la revendication 1 caractérisé en ce qu'il peut établir plusieurs sessions de communication RF simultanément.

33. Dispositif portable suivant la revendication 1 caractérisé en ce que le moyen de communication RF est inactif et ne consomme pas ou très peu d'énergie avant que la communication OSC n'est été établie.

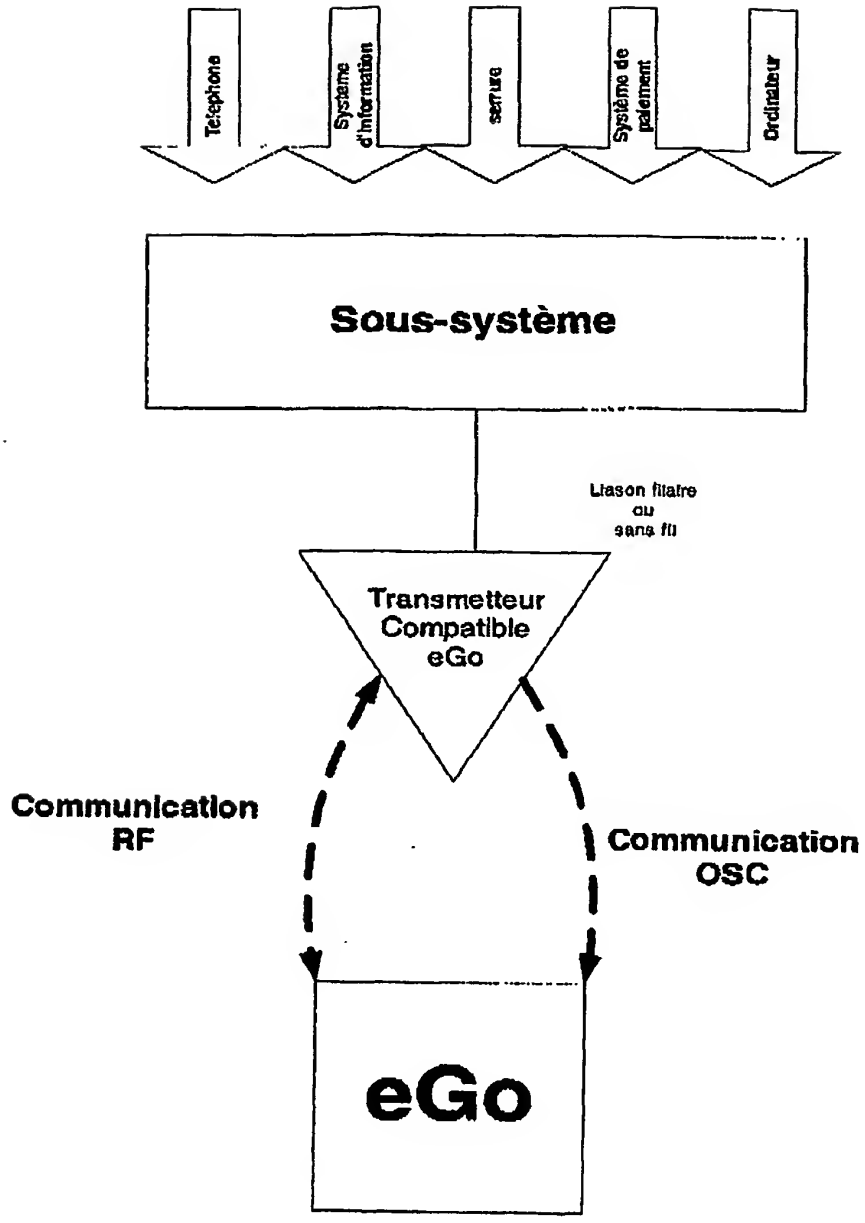

Figure 1-Systeme eGo

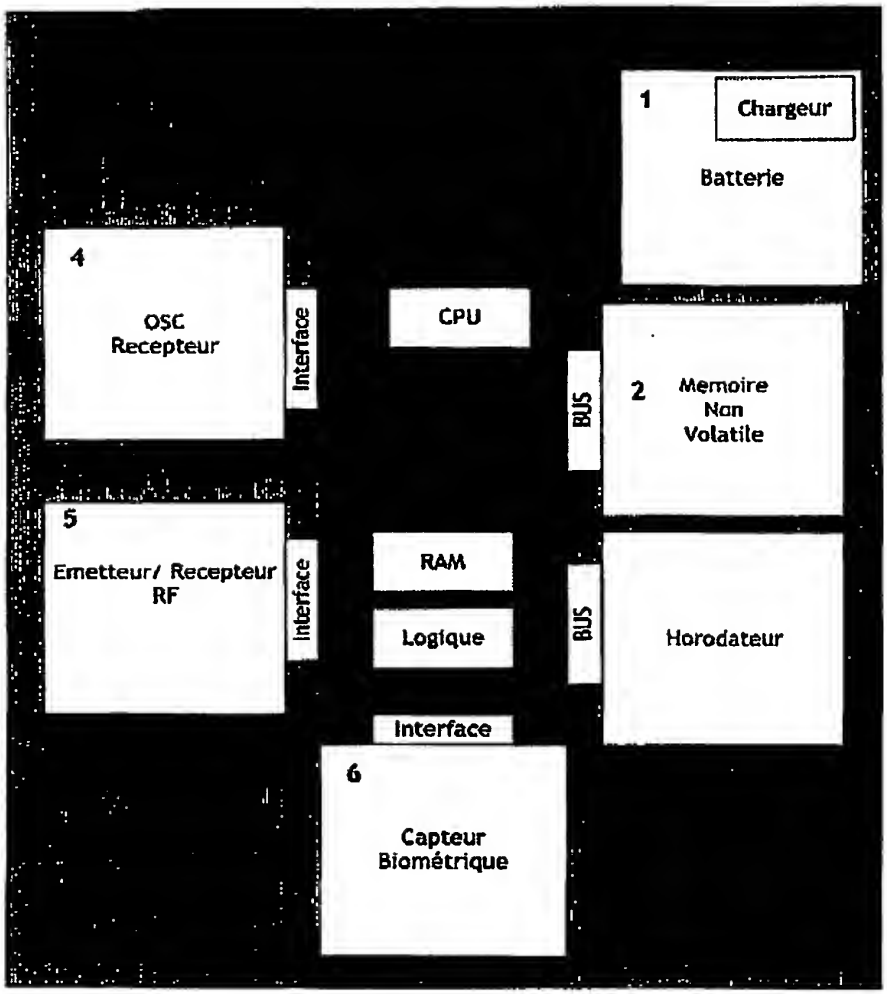

Figure 2-Vue fonctionnelle

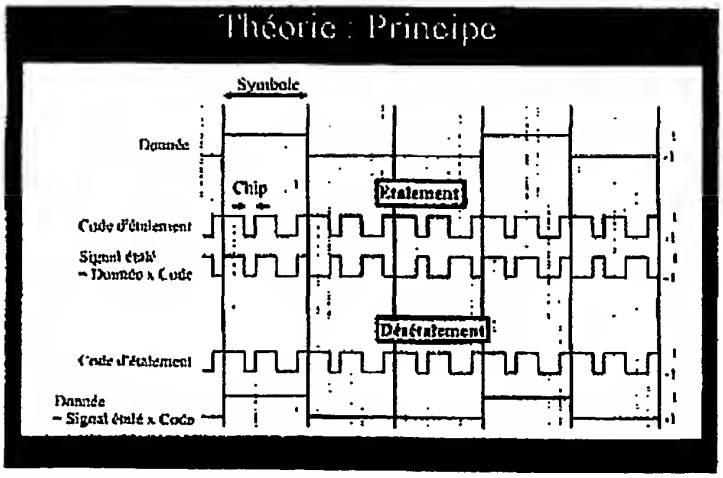

Figure 3-Etalement de spectre

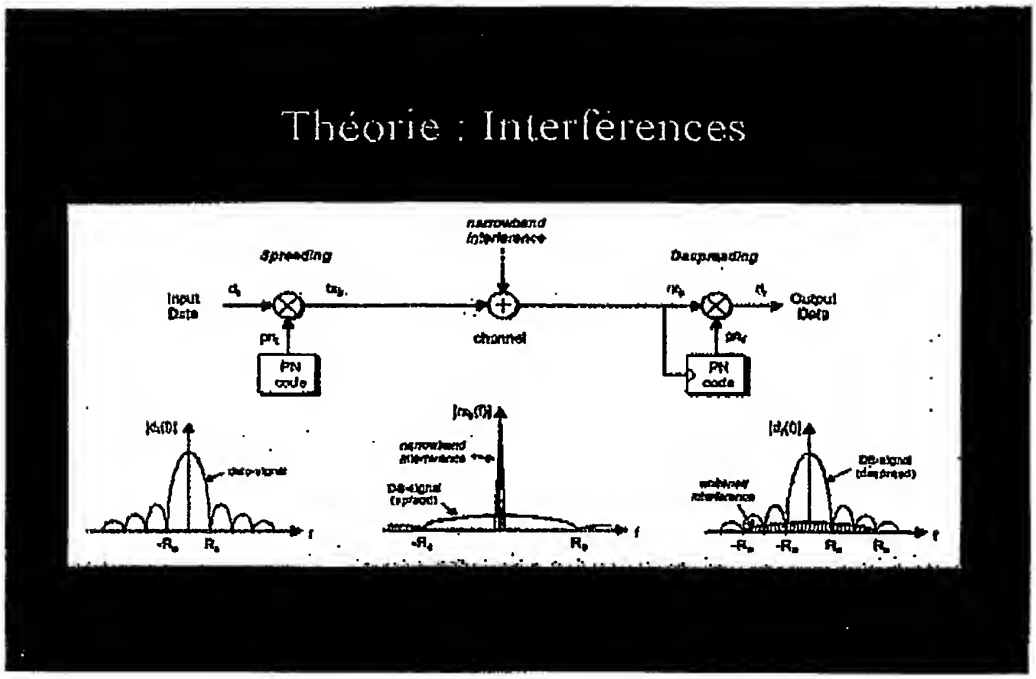

Figure 4-Interférences

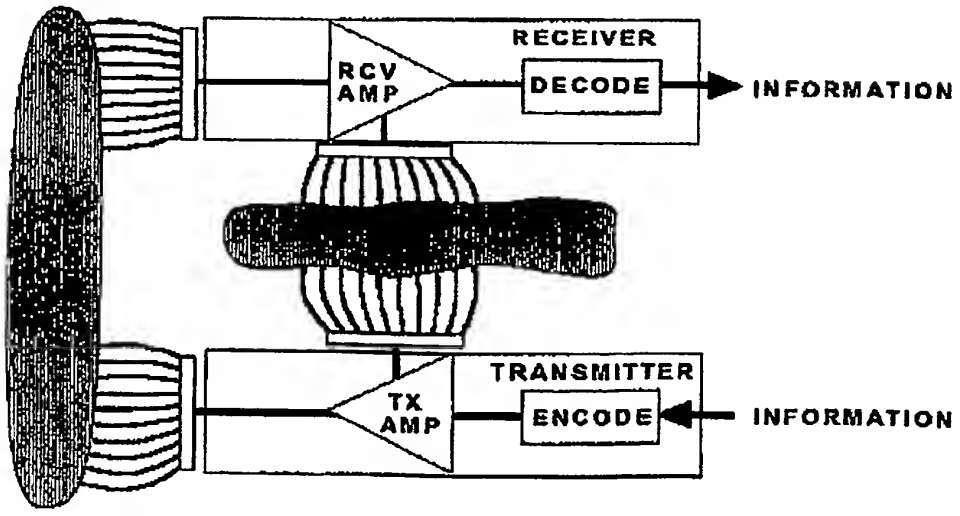

Figure 5-Transmission intra corporelle

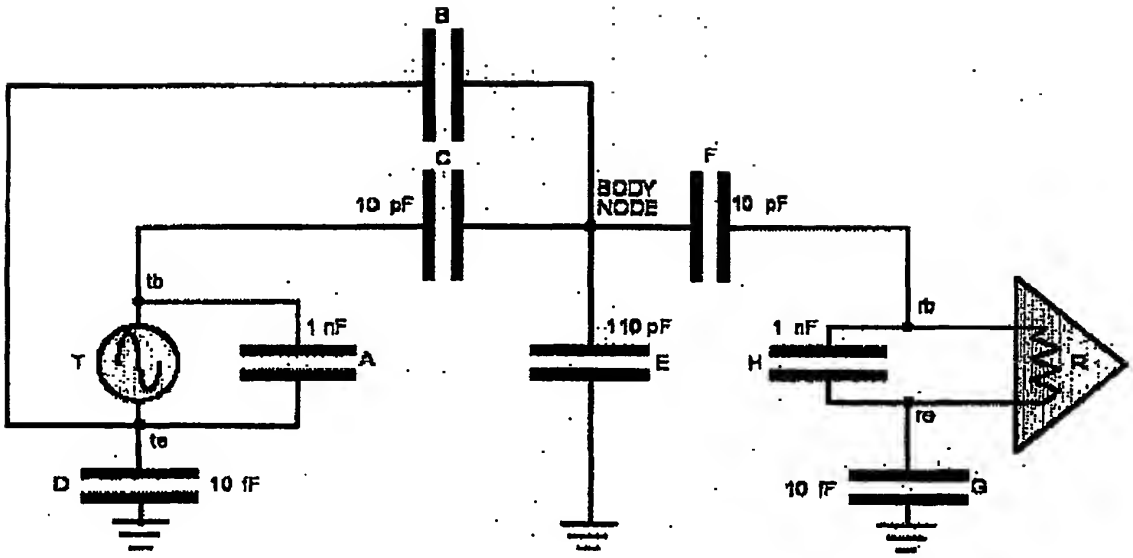

Figure 6-Modèle électrique équivalent

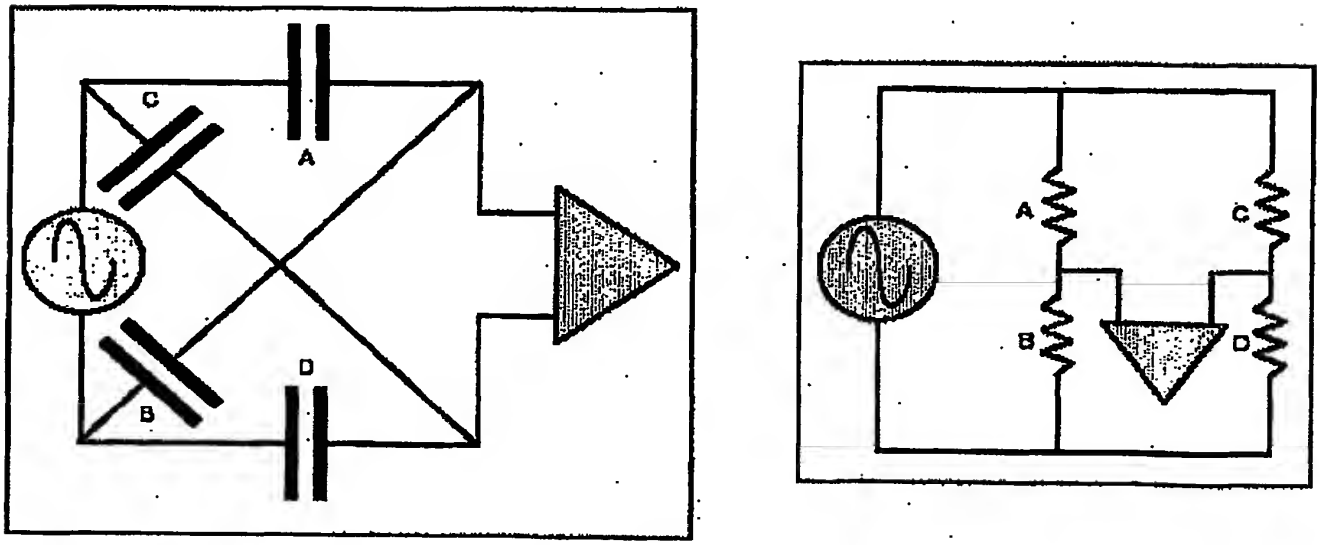

Figure 7-Modèle électrique simplifié

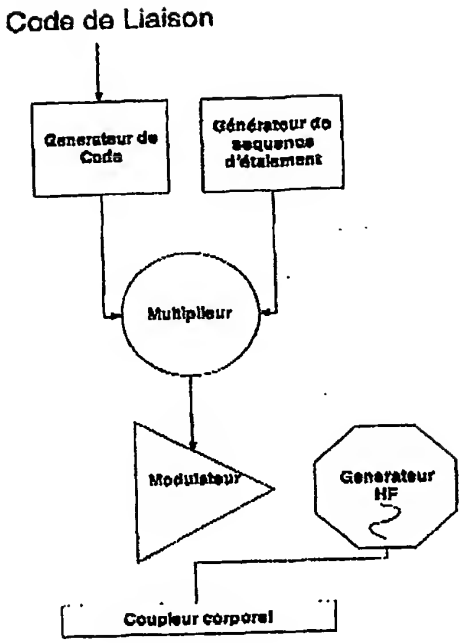

Figure 8-Emetteur OSC